УДК 004.056

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ОПТИМАЛЬНОГО РАСПРЕДЕЛЕНИЯ ЗАЩИТНЫХ РЕСУРСОВ ПО ИСТОЧНИКАМ ИНФОРМАЦИОННЫХ УГРОЗ

© 2019 В. И. Свиридов, С. И. Моисеев

Воронежский институт высоких технологий г. Воронеж, Россия)
ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова»
Воронежский филиал г. Воронеж, Россия)

В работе рассмотрены математические модели, позволяющие оптимально распределить имеющиеся ресурсы защиты информационных систем от угроз разного типа. Применены методы решения оптимизационных задач: линейное программирование, распределительная задача о назначениях, теория игр.

Ключевые слова: информационная безопасность, защита информации, математическое моделирование, распределительные задачи, теория игр.

В связи с интенсивным развитием информационных технологий в последнее время также интенсивно увеличивается количество разного рода видов информационных угроз. В связи с этим разработано большое количество способов защиты систем от вредоносных воздействий, которые, как правило, являются комплексными, позволяющими в той или иной мере обезопасить систему от разных типов информационных угроз, воздействующих по различным каналам. Поэтому, в последнее время актуальным становится вопрос об оптимальном распределении защитных средств и ресурсов по возможным каналам информационного воздействия на систему. Подобные задачи решались с использованием методов прогнозирования [1], с использованием теории латентных переменных [2, 3], и некоторые другие, но относились к узким сферам применения.

В данной работе рассматриваются некоторые математически модели решения задачи оптимальной организации информационной безопасности произвольных систем для случая информационной угрозы по дискретным каналам воздействия на систему.

1. Модели линейного программирования

Рассмотрим следующую модель. На некоторую систему *S* воздействуют *m* видов угроз информационной безопасности, каждая из которых может причинить ущерб, риск которого составляет R_j, $j = 1,2,...,m$. Для защиты системы используются некоторые средства, которые назовем каналами защиты, и число которых равно *n*. Рассмотрим сначала ситуацию, когда каждый канал защиты имеет определенный ограниченный ресурс, который может в определенных пропорциях распределяться между разного вида угрозами. В качестве ресурсов можно рассматривать, например, финансовые, материальные, материальные и др. затраты, направленные на обеспечения защиты по тому ими иному каналу от определенной угрозы. Обозначим B_i – суммарные ресурсы *i*-го канала защиты.

Каждый канал защиты может в той или иной мере (пропорционально доли ресурса, направленного на это) устранить угрозу каждого вида, уменьшив риск. Обозначим $R_{ij}^{'}$, $i = 1,2,...,n$, $j = 1,2,...,m$ – ущерб, нанесенной системе *j*-й угрозой в случае, если она в некоторой степени защищена *i*-м каналом защиты, а $\Delta R_{ij} = R_i - R_{ij}^{'}$ – эффективность от защиты угроз, связанные с работой каналов защиты. Будем считать эффективности от защиты угрозы несколькими каналами защиты аддитивными. Пусть в случае, когда единица ресурса *i*-го канала защиты направлена на ликвидацию *j*-й угрозы, эффективность составит a_{ij}. Если обозначить x_{ij} – количество ресурсов *i*-го канала защиты направленных на *j*-ю угрозу, то $\Delta R_{ij} = a_{ij} x_{ij}$. Общая эффективность защиты

Свиридов Владислав Иванович – Воронежский институт высоких технологий, магистрант, vladsviridov2008@yandex.ru.
Моисеев Сергей Игоревич – Воронежский филиал ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова», доцент кафедры информационных технологий в экономике, к. ф-м, доцент, moiseev@nxt.ru.

всей системы составит $\Delta R = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_{ij}$.

Необходимо найти такое распределение ресурсов каналов защиты по угрозам, чтобы суммарная эффективность была максимальна. Если возможное суммарное количество ресурсов всех каналов защиты, направленных на определенную угрозу неограниченно, то получаем задачу линейного программирования [4]:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_{ij} \to \max;$$

$$\sum_{j=1}^{m} x_{ij} \le B_i, \qquad i = 1,2,...,n$$

$$x_{ij} \ge 0, \quad i = 1,2,...,n; \quad j = 1,2,...,m.$$

Если суммарное количество ресурсов всех каналов защиты, направленных j-ю угрозу ограниченно величиной C_j, то добавиться дополнительное ограничение $\sum_{i=1}^{n} x_{ij} \le C_j, \qquad j = 1,2,...,m$. Решение задачи можно найти симплекс-методами либо на ЭВМ [5].

2. Задача о назначениях

Это частный случай модели, описанной выше, но ввиду своей специфики и в связи с частой применимостью на практике, ее рассматривают отдельно под названием «Задача о назначениях» [6]. Предположим, что каждый канал защиты может быть направлен на одну и только одну угрозу, и каждая угроза должно защищаться не менее чем одним каналом защиты.

Введем переменные x_{ij} – факт назначения или неназначения i-го канала защиты на j-ю угрозу, которая определяется по правилу:

$$x_{ij} = \begin{cases} 0, \ \textit{если} \ \ i-\textit{й} \ \ \textit{канал} \ \ \textit{не} \\ \quad \textit{защищает} \ \ j-\textit{ю} \ \ \textit{угрозу}; \\ 1, \ \textit{если} \ \ i-\textit{й} \ \ \textit{канал} \\ \textit{защищает} \ \ j-\textit{ю} \ \ \textit{угрозу}. \end{cases}$$

Тогда математическая модель задачи есть:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} R'_{ij}x_{ij} \to \max;$$

$$\begin{cases} \sum_{j=1}^{n} x_{ij} = 1, \ (i = 1,2,...,n); \\ \sum_{i=1}^{m} x_{ij} \ge 1, \ (j = 1,2,...,m); \end{cases}$$

$$0 \le x_{ij} \le 1; \quad x_{ij} - \textit{целое}.$$

Если число каналов защиты равно числу угроз $n=m$, то знак неравенства во второй группе ограничений заменяется на знак равенства. Задача о назначениях может быть решена аналитически, например, венгерским методом [7] или численно на ЭВМ.

3. Модели теории игр

Этот класс моделей позволяет принимать оптимальные решения в условиях конфликта. Под конфликтом понимается ситуация, когда в участники противоборства: *Методы вредоносной атаки* ↔ *Методы защиты* выбирают свои действия осознанно с учетов возможных противодействий другой стороны так, чтобы максимизировать свой выигрыш. Эти участники называются игроками, а выбранные ими действия при противоборстве – стратегиями. Будем считать организатора защиты – игроком А, а организатора информационных угроз – игроком В.

Пусть игрок А имеет n стратегий защиты от информационных угроз: $A_1, A_2, \ldots, A_n$, и каждая стратегия защиты имеет ту или иную эффективность для каждой стратегии $B_1, B_2, \ldots, B_m$ из m возможных информационных угроз игроком В. Эти эффективности обозначим a_{ij}.

Каждый игрок может смешивать свои возможные стратегии, частично реализовывая несколько из них в определенных долях. Пусть p_i – доля стратегии защиты A_i, а q_i – доля стратегии угрозы B_i. Тогда для нахождения этих долей необходимо решать прямую и двойственную задачи линейного программирования вида:

$$x_1 + x_2 + ... + x_n \to \min;$$

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + ... + a_{n1}x_n \geq 1; \\ a_{12}x_1 + a_{22}x_2 + ... + a_{n2}x_n \geq 1; \\ \quad\quad ... \\ a_{1m}x_1 + a_{2m}x_2 + ... + a_{nm}x_n \geq 1; \end{cases}$$

$$x_i \geq 0; \;\; i = 1,2,...,n.$$

$$y_1 + y_2 + ... + y_m \to \max;$$

$$\begin{cases} a_{11}y_1 + a_{12}y_2 + ... + a_{1m}y_m \leq 1; \\ a_{21}y_1 + a_{22}y_2 + ... + a_{2m}y_m \leq 1; \\ \quad\quad ... \\ a_{n1}y_1 + a_{n2}y_2 + ... + a_{nm}y_m \leq 1 \end{cases}$$

$$y_j \geq 0; \;\; j = 1,2,...,m.$$

Из решения задач линейного программирования находится общая эффективность защиты системы

$$\Delta R = \frac{1}{x_1 + x_2 + ... + x_n} = \frac{1}{y_1 + y_2 + ... + y_m}$$ и доли каждой стратегии обоих игроков $p_i = \Delta R \cdot x_i, \;\; q_j = \Delta R \cdot y_j$.

Следует отметить, что описанные методы позволяют найти не только наиболее эффективную защиту от информационных угроз, но и организацию наиболее эффективного вредоносного воздействия на систему.

ЛИТЕРАТУРА

1. Менжулин, Р. В. Управление эффективностью защиты информации в распределенных платежных системах на основе банковских карт / Р. В. Менжулин, С. И. Моисеев // Вестник Воронежского государственного технического университета, 2011. – Т. 7. – № 7. – С. 95-98

2. Моисеев, С. И. Модель оценки качества программного обеспечения, основанная на методе Раша оценки латентных переменных / С. И. Моисеев, Ю. В. Черная, Е. В. Паршина // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – № 1. – 2016. – С. 102-109.

3. Белокуров, С. В. Многокритериальное оценивание безопасности объектов инфокоммуникационных систем с учетом влияния латентных параметров / С. В. Белокуров, Р. В. Кузьменко, С. И. Моисеев, Е.О. Окунева // Вестник Воронежского института ФСИН России. – № 4. – 2016. – С. 39-45

4. Вентцель, Е. С. Исследование операций. Задачи, принципы, методология / Е. С. Вентцель. – М.: Наука, 1980.

5. Моисеев, С. И. Математические методы и модели в экономике. Учебное пособие / С. И. Моисеев, А. В. Обуховский. – Воронеж: АОНО ВПО "Ин-т менеджмента, маркетинга и финансов". – Изд. 2-е, испр., 2009. – 160 с.

6. Окунева, Е. О. Методы оптимальных решений: учебное пособие / Е. О. Окунева, С. И. Моисеев // Воронеж, ВФ МГЭИ, 2013. – 139 с.

7. Вагнер, Г. Основы исследования операций. – М.: Мир, 1972.

MATHEMATICAL MODELS OF OPTIMAL DISTRIBUTION OF PROTECTIVE RESOURCES BY SOURCES OF INFORMATION THREATS

© 2019 V. I. Sviridov, S. I. Moiseev

Voronezh Institute of High Technologies (Voronezh, Russia)
Voronezh branch of the Plekhanov Russian University of Economics (Voronezh, Russia)

The paper considers the mathematical models that allow optimal distribution of the available resources to protect information systems from threats of various types. The methods for solving optimization problems are used: linear programming, the distribution task of assignments, game theory.

Key words: information security, information protection, mathematical modeling, distribution problems, game theory.